

2 **FIELD OF INVENTION**

3 The present invention relates to management of access
4 to a database which stores confidential personal data. It
5 is more specifically directed to access management to effec-
6 tuate reliable and high-speed processing. It also relates
7 to access management for a registrant database storing
8 personal data through a network while maintaining
9 confidentiality.

10 **BACKGROUND OF THE INVENTION**

11 In recent years, there are many cases where personal
12 data such as client data or resident data are stored and
13 saved in a database. Especially, as a network such as the
14 Internet is put into general use, personal data such as
15 privacy data will be accumulated in a registrant database
16 installed in one management site. Access to the database
17 storing an enormous amount of private data must be managed
18 at a high security level so as to prevent unauthorized
19 leakage of the highly confidential personal data.
20 Therefore, various access management techniques have been
21 offered heretofore.

22 For example, a situation is assumed in such a way that
23 a company, a local government, or a national government
24 (hereinafter referred to as a policy setter) collects regis-
25 trant data of clients, residents, companies, or organiza-
26 tions (regardless of being commercial or noncommercial;

1 hereinafter simply referred to as registrants) and saves the
2 respective registrant data in a database. At this time, the
3 data saved in the database needs to be treated at a high
4 security level from the viewpoints of privacy protection and
5 prevention of unlawful acts such as unlawful acquisition of
6 right.

7 For this reason, the policy setter normally sets a
8 policy concerning treatment of the collected registrant data
9 as a privacy policy. This privacy policy may include
10 descriptions as to who can use which information out of the
11 collected registrant data for what purpose, for example.
12 The policy setter facilitates processing for an operation
13 data, while collecting the registrant data, so that a person
14 who desires member registration may confirm the privacy
15 policy set up by the policy setter, to input the privacy
16 data by mutual agreement. When the policy setter treats the
17 registrant data, it is considered necessary to arrange a
18 mechanism to protect the registrant data by means of check-
19 ing whether or not the responsible person in charge who
20 intends to access the database has a proper access right so
21 as to eliminate any access not satisfying the privacy policy
22 concerning the registrant data.

23 SUMMARY OF THE INVENTION

24 Thus, an aspect of the present invention is to provide
25 access management methods and systems wherein privacy needs
26 are taken into consideration. That is, an aspect of the
27 present invention is to provide an access management system,
28 an access management method, a control program for causing a
29 computer to execute the access management method, and a
30 computer-readable recording medium recording the control
31 program, which ensures access to highly confidential data

1 such as privacy data of registrants with high reliability
2 and at a high security level.

3 Another aspect of the present invention is to provide
4 an access management system and an access management method
5 necessary for the above-described access management through
6 a network.

7 In order to attain the above-described aspects, and
8 focusing on the fact that privacy policies can be classified
9 into elements depending on a policy setter and elements
10 depending on registrants. The present invention is provided
11 based on an idea that appropriateness checks with a regis-
12 trant database using an authorization engine can be acceler-
13 ated without degrading a security level, when it is possible
14 to calculate access authorization data in advance and to
15 adapt a calculated result to an access authorization by
16 means of organizing the above-mentioned elements into
17 independent lists or tables.

18 In an access management method according to an example
19 embodiment of the present invention, access types for access
20 to a registrant database is decided by using the elements
21 dependent on the policy setter divided into data usage type
22 by the person in charge (a data user) in the policy setter,
23 and a business purpose type. In this way, an access type
24 list to be used as the access authorization data is gener-
25 ated and stored in a storage area in advance.

26 Regarding the elements depending on the registrants, a
27 cluster identification value for each registrant is regis-
28 tered based on condition data of an arbitrary number set by
29 the registrant. In this way, a registrant condition table
30 to be used as the access authorization data is generated.
31 In the access management method according to this embodiment
32 of the present invention, the access type is decided when
33 the authorization engine receives an access request from an
34 application. The authorization engine searches the access

1 type list based on the decided access types, and obtains a
2 consent pattern corresponding to the condition data.

3 Furthermore, according to the present invention, there
4 is provided an access controlling method for controlling a
5 computer to manage access to registrant data through a
6 network. Here, the access management method includes the
7 steps of: causing an authorization engine to use access
8 authorization data calculated in advance through the
9 network; causing the authorization engine to receive an
10 access request from outside to a registrant database storing
11 the registrant data containing privacy of the registrant;
12 deciding an access type upon receipt of the access request
13 from the outside; and controlling the access to the regis-
14 trant database by comparing the decided access type with the
15 access authorization data decided prior to the access
16 request.

17 **BRIEF DESCRIPTION OF THE DRAWINGS**

18 For a more complete understanding of the present
19 invention and the advantages thereof, reference is now made
20 to the following description taken in conjunction with the
21 accompanying drawings.

22 Figs. 1A and 1B are views showing data configurations
23 for reference as privacy policies in an embodiment of the
24 present invention.

25 Figs. 2A to 2C are views showing data structures of an
26 access type list and a registrant condition list which
27 constitute access authorization data created in an access
28 management system according to an example embodiment of the
29 present invention.

30 Fig. 3 is a flowchart of the access management method

1 according to the example embodiment of the present
2 invention.

3 Fig. 4 is a flowchart showing a modified example of
4 the access management method according to the example
5 embodiment of the present invention shown in Fig. 3.

6 Fig. 5 is a view showing a restructuring example of
7 the privacy policy to generate the access authorization data
8 used in an access management method according to a second
9 embodiment of the present invention.

10 Fig. 6 is a view showing reference axes to be applied
11 when performing compression processing of a registrant
12 condition table contained in the access authorization data
13 which are usable in the access management method of the
14 present invention.

15 Fig. 7 is a view schematically showing compression
16 processing along an access type axis in the present
17 invention.

18 Fig. 8 is a flowchart showing processing to be
19 executed by an authorization engine when executing the
20 access management method of the present invention by use of
21 the data compression shown in Fig. 7.

22 Fig. 9 is a schematic diagram showing compression
23 processing along a condition data axis, which is another
24 embodiment of the data compression method in the present
25 invention.

26 Fig. 10 is a flowchart showing processing to be
27 executed by the authorization engine when using the access
28 authorization data after execution of the compression
29 processing along the condition data axis.

30 Figs. 11A to 11C are views showing an outline of data
31 compression processing along a registrant axis which is used
32 in the present invention.

33 Fig. 12 is a flowchart showing the processing for
34 adding and updating the access authorization data at

1 runtime, which can be executed when using the access
2 authorization data in the access management method according
3 to the second embodiment of the present invention.

4 Fig. 13 is a flowchart showing primary processing of
5 the access management method of the present invention until
6 start of the processing of the access management method.

7 Fig. 14 is a view showing the preferred embodiment in
8 which the registrant condition table is not created in
9 advance but added dramatically.

10 Fig. 15 is a view showing the preferred embodiment in
11 which a record is added dramatically when the registrant
12 condition table is created for each access type in the
13 access management method of the second embodiment of this
14 invention.

15 Fig. 16 is a schematic functional block diagram
16 showing an access management system according to the present
17 invention where the access management method of the present
18 invention is implemented.

19 Fig. 17 is a view showing an access management system
20 according to a second embodiment of the present invention.

21 Fig. 18 is a view showing an access management system
22 according to a third embodiment of the present invention.

23 Fig. 19 is a view showing a conventional access
24 management system.

25 Fig. 20 is a view showing a data flow in the conven-
26 tional access management system.

27 DESCRIPTION OF THE INVENTION

28 The present invention provides methods systems and
29 apparatus for access management wherein privacy needs are
30 taken into consideration. Figure 19 shows an example of a
31 conventional access management system in which the privacy

1 needs to be taken into consideration. In Figure 19, an
2 authorization engine 104 is disposed between an application
3 100 and a registrant database 102. A person in charge, such
4 as the policy setter, accesses the registrant database 102
5 through the application 100. Upon receipt of an access
6 request from the person in charge, the authorization engine
7 104 makes reference to a privacy policy database 106 and
8 judges the access right of the person in charge. In this
9 way, the access management system is intended to prevent
10 free and direct access to the registrant database by the
11 person in charge without being checked whether or not having
12 a proper access right. Concrete processing of the authori-
13 zation engine 104 shown in Figure 19 will be explained. When
14 the authorization engine 104 receives the access request to
15 registrant information from the application 100, the
16 authorization engine 104 judges whether or not the access
17 request satisfies the privacy policy. Moreover, when the
18 authorization engine 104 judges that the access request
19 satisfies the privacy policy, the authorization engine 104
20 facilitates a series of data processing that permits the
21 person in charge to access the registrant database, enabling
22 the person in charge to obtain registrant data, and return-
23 ing the registrant data to the application.

24 As described above, it is possible to prevent the
25 misuse of the privacy information of the registrants by
26 judging whether or not the received access request satisfies
27 the privacy policy in real time with the authorization
28 engine 104. Hereafter, whether or not the access request
29 satisfies the private policy will be checked or judged
30 referring to "appropriateness check" in this invention.
31 Consequently, judgment of satisfaction and subsequent
32 issuance of an access permit will be hereinafter referred to
33 as "authorization". On the contrary, non-issuance of the
34 access permit or generation of an access disapproval signal

1 will be hereinafter referred to as "disapproval".

2 In comparison with a usual access management system
3 configured to access the registrant database 102 directly
4 without using the authorization engine 104, access to the
5 registrant database 102 through the authorization engine 104
6 as shown in Figure 19 has a processing of "appropriateness
7 check" added to the access management system.

8 Figure 20 shows a concrete example of data and
9 processing to be used for the appropriateness check of the
10 above-described privacy policy. In order to describe the
11 conventional appropriateness check of the privacy policy
12 shown in Figure 19 more concretely, an operation that the
13 policy setter sends direct mails (DM) will be taken into
14 consideration in Figure 20. Here, if assuming the situation
15 such that a person in charge for marketing at the policy
16 setter intends to obtain data of names and addresses of
17 registrants satisfying a condition of "registrants with ages
18 of 30 years or older and having addresses in xxx" out of the
19 registrant database for the purpose of marketing of its own
20 product, and the registrant database 102 is a relational
21 database, an application execution unit 100 issues an access
22 request in a format such as an SQL sentence to the authori-
23 zation engine 104 with the condition that "registrants with
24 ages of 30 years or older and having addresses in xxx", then
25 at this time, in addition to the SQL sentence, the access
26 request may further include information such as person-in-
27 charge identification data (a real name such as "Mr. A in
28 charge of marketing", an employee code, a password, or a
29 user ID, for example), a type of registrant data required to
30 be accessed ("a name, an address, a telephone number, and a
31 fax number", for example), a type of business which is the
32 purpose of access (a "campaign", for example), which are
33 necessary for the appropriateness checks.

34 When receiving the access request, the authorization

1 engine 104 executes the SQL sentence and receives a list of
2 "names" and "addresses" of all registrants satisfying the
3 condition of "registrants with ages of 30 years or older and
4 having addresses in xxx". Next, the authorization engine
5 104 searches all the policies to be evaluated with the
6 privacy policy database 106 and thereby obtains policy data.
7 Subsequently, the following procedures take place depending
8 on each piece of the obtained registrant data. First, if
9 assuming that there are 10,000 results for the words in the
10 registrant data satisfying the condition of "registrants
11 with ages of 30 years or older and having addresses in xxx"
12 as a search result, the following calculations (1) and (2)
13 will be executed concerning the "names" and the "addresses"
14 of those 10,000 records.

15 (1) All the privacy policies to be evaluated are
16 evaluated. At this time, if there are conditions other
17 than the policies to be arbitrarily set by the regis-
18 trants, then data necessary for judgment of the condi-
19 tions are obtained in the course of evaluation of the
20 privacy policies. For example, it may be necessary to
21 retrieve the condition data recording an agreement of
22 the registrants out of the registrant database and
23 check whether or not the registrants have agreed in
24 receiving DMs.

25 (2) A final evaluation result is calculated based on
26 an evaluation result of the privacy policies to be
27 evaluated. As a condition data logic for calculating
28 the final evaluation result may include a variety of
29 logic, such as AND logic which authorizes only when all
30 the policies are OK, OR logic which authorizes when
31 there is at least one policy is OK, and the like. In
32 aggregate, such judgment processing will be repeated by

1 20,000 times at the maximum including the processing
2 for the calculations (1) and (2).

3 That is, when the appropriate checks are carried out
4 in the access management system shown in Figure 19 and
5 Figure 20, the overhead attributable to the processing for
6 the appropriateness checks becomes an issue. Particularly,
7 in the case of an application which accesses an enormous
8 volume of registrant data at once, such as data mining by
9 use of the registration database or an application for
10 sending electronic mails or DMs as a part of a promotion
11 campaign, the overhead becomes a more serious problem as the
12 number of registrants climes. Therefore, serious problems
13 are raised over operation efficiency on the policy setter
14 side.

15 Therefore, there has been a demand for access manage-
16 ment with high reliability and at a high security level with
17 respect to highly confidential data such as the privacy data
18 of the registrants.

19 The present invention overcomes the inconveniences
20 described. That is, it provides an access management
21 system, an access management method, a control program for
22 causing a computer to execute the access management method,
23 and a computer-readable recording medium recording the
24 control program, which ensures access to highly confidential
25 data such as privacy data of registrants with high reliabil-
26 ity and at a high security level. Also provided is an
27 access management system and an access management method
28 necessary for the above-described access management through
29 a network.

30 In order to attain these, the invention focuses on the
31 fact that privacy policies can be classified into elements
32 depending on a policy setter and elements depending on
33 registrants. The present invention is based on an idea that

1 appropriateness checks with a registrant database using an
2 authorization engine can be accelerated without degrading a
3 security level, when it is possible to calculate access
4 authorization data in advance and to adapt a calculated
5 result to an access authorization by means of organizing the
6 above-mentioned elements into independent lists or tables.

7 In an access management method according to a example
8 embodiment of the present invention, access types for access
9 to a registrant database is decided by using the elements
10 dependent on the policy setter divided into data usage type
11 by the person in charge (a data user) in the policy setter,
12 and a business purpose type. In this way, an access type
13 list to be used as the access authorization data is gener-
14 ated and stored in a storage area in advance.

15 Meanwhile, regarding the elements depending on the
16 registrants, a cluster identification value for each regis-
17 trant is registered based on condition data of an arbitrary
18 number set by the registrant. In this way, a registrant
19 condition table to be used as the access authorization data
20 is generated. In the access management method according to
21 the example embodiment of the present invention, the access
22 type is decided when the authorization engine receives an
23 access request from an application. The authorization
24 engine searches the access type list based on the decided
25 access types, and obtains a consent pattern corresponding to
26 the condition data. The cluster identification value to be
27 authorized by the access type is searched by use of this
28 consent pattern as a key. Discovery of the cluster identi-
29 fication value in the access authorization data includes the
30 steps of instructing access authorization, obtaining the
31 registrant data corresponding to the cluster identification
32 value from the registrant database, and returning the regis-
33 trant data to the application. Moreover, in the above-
34 described configuration of the present invention, it is

1 possible to use a method for dynamically constructing the
2 access authorization data such as the access type list or
3 the registrant condition table by allowing a high-speed
4 access memory such as a cache memory to sequentially update
5 the access authorization data at runtime.

6 Meanwhile, an access management method according to a
7 second embodiment of the present invention uses access
8 authorization data with a different configuration. The
9 access authorization data includes an access type list
10 generated by use of the data usage type and the business
11 purpose type. The access authorization data used in the
12 access management method according to the second embodiment
13 of the present invention includes the access type list and a
14 registrant condition table, in which elements of a policy
15 setter and elements of the registrants are functionally
16 separated at a higher level than the level in the above-
17 described example embodiment. Moreover, the access authori-
18 zation data used in this access management method includes
19 the registrant condition table in a format configured to
20 exclude data not accessed from the access authorization data
21 corresponding to the access type and belonging to the access
22 type respectively. Simultaneously, in the access management
23 method according to the second embodiment of the present
24 invention, it is possible to use a so-called compressed
25 registrant condition table in addition to an authorization
26 list where everything is authorized to be accessed and a
27 disapproval list where everything is disapproved to be
28 accessed. It is possible to compress the registrant condi-
29 tion table configured according to the second embodiment of
30 the present invention based on a prescribed rule for a
31 condition agreed by the registrant upon registration.
32 Accordingly, the registrant condition table can achieve high
33 speed while securing a high security level.

34 That is, according to the present invention, there is

1 provided an access management system for managing access to
2 registrant data including an authorization engine for
3 controlling access to a registrant database storing regis-
4 trant data having privacy data of a registrant and for
5 controlling access to the registrant database by use of a
6 prescribed privacy policy and condition data designated by
7 the registrant. Here, the authorization engine includes an
8 authorization judgment unit for deciding an access type from
9 an access request received from outside and for controlling
10 reference to the registrant database based on the access
11 request by use of access authorization data to be decided
12 prior to the access request in connection with the access
13 type of the registrant data.

14 The above-described access management system of the
15 present invention may further include a preliminary calcula-
16 tion unit for calculating the access authorization data in
17 advance, and a storage area for storing the access authori-
18 zation data. The access authorization data of the present
19 invention may include an identification value for executing
20 access authorization which is generated in advance from the
21 privacy policy and the condition data.

22 The above-described access authorization data of the
23 present invention may further include a table which is
24 generated in advance by use of the privacy policy and the
25 condition data. Moreover, the table may be written in a
26 format to exclude the access authorization data which are
27 not accessed in response to the above-described access type
28 or the condition data of the registrant. The access
29 authorization data of the present invention may further
30 include an authorization list and a disapproval list.

31 According to the present invention, there is provided
32 an access management method for managing access to regis-
33 trant data by use of a computer system. Here, the method
34 includes the steps of: causing an authorization engine to

1 receive an access request from outside; causing the authori-
2 zation engine to decide an access type from the access
3 request; reading access authorization data to be decided
4 prior to the access request in connection with the access
5 type of the registrant data and comparing the access
6 authorization data with the access type; and controlling
7 reference to a registrant database associated with the
8 access request based on the comparison.

9 According to the present invention, there is also
10 provided a computer-executable program for causing a
11 computer to execute the above-described access management
12 method. Moreover, according to the present invention, there
13 is provided a computer-readable recording medium storing the
14 above-described computer-executable program.

15 Moreover, according to the present invention, there is
16 provided an access management system for managing access to
17 registrant data through a network. Here, the access manage-
18 ment system includes: a network; a registrant database
19 storing the registrant data containing privacy of a regis-
20 trant; an application execution unit for issuing access
21 request to the registrant database; an authorization engine
22 connected to the network for controlling the access to the
23 registrant database by receiving the access request from the
24 application unit and using the prescribed privacy policy and
25 condition data designated by the registrant, then control-
26 ling the access to the registrant database and a management
27 server for generating access authorization data to be
28 decided prior to the access request in connection with an
29 access type and for causing the authorization engine to use
30 the access authorization data.

31 According to the present invention, there is provided
32 an access controlling method for controlling a computer to
33 manage access to registrant data through a network. Here,
34 the access management method includes the steps of: causing

1 an authorization engine to use access authorization data
2 calculated in advance through the network; causing the
3 authorization engine to receive an access request from
4 outside to a registrant database storing the registrant data
5 containing privacy of the registrant; deciding an access
6 type upon receipt of the access request from the outside;
7 and controlling the access to the registrant database by
8 comparing the decided access type with the access authoriza-
9 tion data decided prior to the access request.

10 Section A: Outline of access management data to be used in
11 access management according to the present invention

12 Various techniques have been known as systems for
13 checking appropriateness of a privacy policy according to
14 the present invention. Such techniques are also applicable
15 to the present invention. More specifically, "IBM Corpora-
16 tion, IBM Tivoli Privacy Manager for e-business Planning
17 Guide Version 1.1, July 2002" can be mentioned as a basic
18 technique of this invention and can be incorporated in this
19 invention as reference. Figs. 1A and 1B show a data
20 configuration which is referred to as a privacy policy in
21 the present invention. As shown in Figure 1A, the privacy
22 policy is classified into a data usage type 10 of a person
23 in charge who is a data user on a policy setter side, a
24 registrant data type 12, a business purpose type 14, and
25 condition data 16 to be set up by a registrant. More
26 specifically, the data usage type 10 is data for registering
27 a data usage aspect of the person in charge, in such as
28 marketing, distribution, or accounting. Meanwhile, the
29 registrant data type 12 is data registering privacy of the
30 registrant, such as an address, a name, an age, a sex, a
31 telephone number, or an electronic mail address. The
32 business purpose type 14 is more specifically data

1 designating a business necessary for access to the regis-
2 trant data from the policy setter side, such as
3 distribution, marketing, or accounting. The condition data
4 16 are data registering a condition agreed and designated by
5 the registrant upon registration as accessible privacy of
6 the registrant.

7 Configurations of respective data will be described by
8 use of Figure 1B as an example. As shown in Figure 1B, if
9 assuming herein that the person in charge on the policy
10 setter side is in charge of processing a distribution
11 business, the person in charge needs the registrant data
12 type "name, address, telephone number" in order to carry out
13 the business. Meanwhile, although various business phases
14 are conceivable for the distribution, the business purpose
15 type of the "distribution" is assumed as "shipping" in
16 Figure 1B. In the case of the "distribution" as shown in
17 Figure 1B, the condition data are not required because a
18 condition is not particularly set up on the privacy policy
19 side, for example. Accordingly, the condition data are
20 marked as "none" in the embodiment shown in Figure 1B. On
21 the contrary, when the data usage type of the person in
22 charge is "marketing", names, addresses, and zip codes are
23 required for sending DMs. On the other hand, it is not
24 necessary to access other registrant data types. If assum-
25 ing that business purpose type when carrying out the market-
26 ing business described in Figure 1B is "campaign", the
27 condition data becomes "consent for sending DMs".

28 The access management method of the present invention
29 focuses attention on the fact that these privacy policies
30 can be classified into elements to be decided depending on
31 the policy setter and elements designated by the
32 registrants. Accordingly, access authorization data are
33 configured in advance and a functional portion for executing
34 authorization processing (hereinafter referred to as an

1 authorization engine) stores the access authorization data
2 which are generated in advance. Although various aspects
3 are conceivable as the access authorization data, a example
4 embodiment of the present invention will be described based
5 on the assumption that the access authorization data are
6 generated as a set of an access type list and a registrant
7 condition table.

8 Figs. 2A to 2C are views showing data structures of
9 the access type list and the registrant condition table
10 constituting the access authorization data to be generated
11 in the access management method according to the example
12 embodiment of the present invention. Figure 2A shows an
13 aspect of the access type list. As shown in Figure 2A, the
14 access type list is classified into the business purpose
15 types, the registrant data types, wherein the condition data
16 corresponds to the respective data usage types. Moreover,
17 in the access type list shown in Figure 2A, access to
18 "addresses, names" and the like are not set up for the
19 registrant data type "distribution", and the consent condi-
20 tion is not set up for the business purpose type "shipping".
21 For this reason, "none" is indicated, which means access is
22 enabled in response to only combination of the data usage
23 type and the business purpose type.

24 Moreover, in the access type list shown in Figure 2A,
25 when the data usage type is "accounting", access to the
26 registrant data type "address" is "disapproved" concerning
27 the business purpose type "accounting" in terms of the
28 privacy policy; that is, the access is disapproved.
29 Furthermore, regarding the data usage type "publicity",
30 access to the registrant data type such as addresses or
31 names is indicated as "condition 1" for "DM posting". More
32 specifically, the "condition 1" is an instruction to make
33 reference to the consent data of the registrants regarding
34 DM posting and to use return values thereof. The access

1 type list shown in Figure 2A may be maintained in a normal
2 table format as shown in Figure 2A, or may be retained as a
3 hash table using "the data usage type [plus] the registrant
4 data type [plus] business purpose type" as a key.

5 Figure 2B is a view showing an aspect of the regis-
6 trant condition table which constitutes the access authori-
7 zation data of the present invention and is stored in an
8 appropriate storage area included in the access management
9 system of the present invention together with the access
10 type list shown in Figure 2A. In the registrant condition
11 table shown in Figure 2B, registrant identifiers (hereinaf-
12 ter referred to as registrant IDs" given to each registrant
13 in the registrant database, a list of the condition data
14 indicating necessities of setting or consent at least by the
15 registrants, and cluster identification values generated
16 from the condition data by use of prescribed logic such as
17 logical addition or logical multiplication are registered
18 for each registrant ID to constitute records. In the
19 particular aspect shown in Figure 2B, the registrant condi-
20 tion table may include appropriate registrant data type
21 other than the above-described database.

22 The condition data to be registered in the registrant
23 condition table shown in Figure 2B are not particularly
24 limited in the present invention. However, the condition
25 data may include data concerning agreement or disagreement
26 to the consent conditions in the privacy policies set by the
27 policy setter, such as reference to names, addresses,
28 telephone numbers, facsimile numbers, ages, sexes,
29 electronic mail addresses, interested fields or preferences.
30 Moreover, the condition data may further include a condition
31 such as age limit, which can be arbitrarily set by the
32 policy setter. The registrant condition table shown in
33 Figure 2B is provided with the cluster identification values
34 A to C which are given to each registrant. The present

1 invention may further adopt other cluster identification
2 values as appropriate. According to the present invention,
3 the cluster value included in the registrant condition table
4 executes access authorization if only the corresponding
5 cluster identification value is discovered.

6 The registrant condition table shown in Figure 2B can
7 be entirely calculated in advance. However, as will be
8 described later, it is also possible to use an aspect in
9 which a registration area is secured in advance; a logic
10 judgment of the condition data is carried out at runtime;
11 and the cluster identification values are judged, to add
12 records in the registration area. In addition, Figure 2C
13 shows an aspect in which the function of the registrant
14 condition table of the present invention shown in Figure 2B
15 is separated into a consent pattern; a table storing the
16 cluster identification values corresponding to the consent
17 pattern using the cluster values as keys; and a table
18 constituted by the registrant IDs and the cluster identifi-
19 cation values. In the aspect shown in Figure 2C, it is also
20 possible to constitute the access authorization data having
21 the similar function to the registrant condition table shown
22 in Figure 2B.

23 Figure 3 shows a flowchart of the access management
24 method according to the example embodiment of the present
25 invention. In the access management method according to the
26 example embodiment of the present invention, in Step S10,
27 the privacy policies are read out of the privacy policy
28 database and the access type list is generated by register-
29 ing the data usage types, the authorizable registrant data
30 types, the business purpose types, and the condition data
31 for reference. In Step S12, the registrant database is
32 accessed to read out the registrant data types and the
33 corresponding condition data thereto, and then the regis-
34 trant condition table is generated so as to include the

1 cluster identification values depending on the consent
2 conditions of the registrants in response to condition logic
3 to be applied to the condition data.

4 In Step S14, the authorization engine receives the
5 access request from the application and starts access
6 control to the registrant database. In Step S16, the data
7 usage type, the registrant data type, and the business
8 purpose type which are included in the access request, and
9 requested by the person in charge at the policy setter, are
10 read out and the access type list is searched. In Step S18,
11 as a consequence of the research, whether or not the access
12 type is authorized is judged. When the access type is
13 included in the access type list (yes), the process contin-
14 ues to Step S20 to obtain the condition data or a set of the
15 condition data in the registrant condition table to be used
16 for judgment. Meanwhile, when it is judged in Step S18 that
17 the access type is not authorized (no), the process is
18 branched off to Step S26 to disapprove the access request
19 from the application.

20 In Step S22, it is judged that whether or not the
21 obtained condition data or the set of the obtained condition
22 data coincide with condition data or a set of condition data
23 when registering the cluster identification values in
24 advance, and the corresponding cluster identification value
25 is obtained. When the cluster identification values are
26 obtained in the course of comparison in Step S22, the regis-
27 trant condition table is referenced in Step S24 and regard-
28 ing the registrant IDs corresponding to the cluster
29 identification values, the registrant data are obtained from
30 the registrant database. Then, the registrant data are
31 returned to the application.

32 Meanwhile, when the corresponding cluster identifica-
33 tion value is not found (no) in the judgment in Step S22,
34 then the process is branched off to Step S26 in this

1 embodiment of this invention designed to execute the
2 preliminary calculation, which is explained in Figure 3, and
3 the access request to the registrant data is disapproved.

4 Figure 4 shows a modified example of the access
5 management method shown in Figure 3. The modified example
6 shown in Figure 4 adopts the configuration in which the
7 authorization engine dynamically updates the registrant
8 condition table at runtime after generation of the access
9 type list. In the modified example shown in Figure 4, an
10 access request from an outside application execution unit is
11 received and an access type is obtained in Step S30. In
12 Step S32, whether or not the obtained access type is
13 included in the access type list is judged. In the judgment
14 of Step S32, when the access type is registered already
15 (yes), the condition data or a set of the condition data are
16 obtained in Step S34. Then, in Step S36, the registrant
17 condition table is read out to obtain consent patterns of
18 the condition data, and whether or not an identical consent
19 pattern is registered therein is judged. In the judgment of
20 Step S36, if the identical consent pattern is found out
21 (yes), then access to the registrant data is authorized in
22 Step S38 to obtain the corresponding registrant data, and a
23 result is returned to the application.

24 Meanwhile, if it is judged that no appropriateness is
25 found in the access type (no) in Step S32, then the process
26 is branched off to Step S46 and access disapproval is
27 notified to the application.

28 Meanwhile, if the identical consent pattern is not
29 found (no) in Step S36, the process continues to Step S42
30 and an appropriateness check as similar to the prior art for
31 the condition data or the set of the condition data obtained
32 in Step S34 is executed by applying the condition logic of
33 the privacy policy at runtime. In Step S44, a value
34 obtained as a result of the appropriateness check is judged.

1 When there is appropriateness (yes), access to the regis-
2 trant database is authorized in Step S46, whereby the corre-
3 sponding registrant data are obtained and the results are
4 returned to the application. Simultaneously, in Step S48, a
5 new cluster value such as "D" is obtained. Then data
6 similar to the data shown in Figure 2B are written in a
7 blank record, which is provided in the registrant condition
8 table in advance, to be capable of corresponding with a
9 future access request at high speed.

10 Meanwhile, when it is judged that there is no appro-
11 priateness in Step S44 (no), the process continues to Step
12 S46 and access disapproval is returned to the application.
13 In the modified example of the present invention shown in
14 Figure 4, it is possible to write the registrant condition
15 table or the access type list in a recording medium such as
16 a hard disk at anytime. However, in the access management
17 method according to the example embodiment of the present
18 invention, it is also possible to read the access authoriza-
19 tion data such as the access type list and the registrant
20 condition table into a cache memory together with the blank
21 record at runtime so as to perform reading and writing
22 access at high speed.

23 Moreover, in another embodiment of the present inven-
24 tion, it is also possible to adopt a configuration in which
25 the processes from Step S42 to Step S48 are applied to the
26 access type list to achieve similar processing so that the
27 access type list is updated at runtime.

28 The above-described modified example of the access
29 management method of the present invention adopts the
30 constitution to register the access authorization data into
31 a high-speed memory as clusters and to execute addition and
32 updating at runtime. Therefore, a new appropriateness check
33 is executed with respect to an unregistered access type or a
34 consent pattern of the condition data. However, the access

1 management method according to the modified example has the
2 following advantages that: (i) it is not necessary to
3 execute processing for configuring the access type list or
4 the registrant condition table in advance; (ii) it is not
5 necessary to perform preliminary calculation for the appro-
6 priateness check for the condition data which are not judged
7 at all or for an access request having considerably low
8 utilization; and (iii) the access management method can deal
9 with updating of the registrant data without adding another
10 process to the system for executing the appropriateness
11 check.

12 Figure 5 is shows a restructuring example for the
13 privacy policy to generate the access authorization data
14 used in the access management method according to the second
15 embodiment of the present invention. In the restructuring
16 example for the privacy policy shown in Figure 5, restruc-
17 turing is performed to level up the separation between the
18 elements on the policy setter's side and the elements on the
19 registrant's side than the restructuring example shown in
20 Figure 1. In Figure 5, access authorization conditions
21 obtained from the privacy policy are restructured as
22 described below. That is, only the policy setter sets and
23 manages the data usage type 10 and the business purpose type
24 14 in principle. Meanwhile, the condition data 16, the
25 registrant data type 12 and a record number 18 are data
26 which can be modified depending on the registrant. For this
27 reason, the access authorization data used in the access
28 management method according to the second embodiment of the
29 present invention adopts the configuration in which the
30 access type list is generated by use of the data usage type
31 10 and the business purpose type 14, and further the regis-
32 trant condition table is generated by use of the condition
33 data 16, the registrant data type 12, and the record number
34 18, and the access type list and the registrant condition

1 data table are calculated in advance as the access authori-
2 zation data and are stored in a prescribed storage area.

3 That is, in the access management method of the
4 present invention shown in Figure 5, the registrant condi-
5 tion table corresponding to the access type and further
6 including the condition data having the same numbers of
7 condition data with the record numbers of the registrants is
8 generated and registered in advance. In the access manage-
9 ment method using the access authorization data shown in
10 Figure 5, when the access type is designated, it is satis-
11 factory if only a value of the relevant condition data in
12 the corresponding registrant condition table is referenced.
13 Therefore, this access management method is common to the
14 access management method according to the example embodiment
15 of the present invention in terms of capability of acceler-
16 ating the appropriateness check compared with the conven-
17 tional access management method, in that it is not necessary
18 to check the appropriateness of the condition data while
19 reading the privacy policy data at runtime and applying the
20 condition logic. Moreover, the access management method
21 shown in Figure 5 can also adopt a modified example where
22 the access authorization data is dynamically added and
23 updated at runtime.

24 On the other hand, when executing the access manage-
25 ment method using the access authorization data shown in
26 Figure 5, it is necessary to store the registrant condition
27 table, which is calculated in advance in terms of the
28 consent patterns of all the access types, into the storage
29 area. To achieve this, an enormous storage area (such as a
30 memory or a database) is required in many cases correspond-
31 ing to the number of the registrants. If the preliminary
32 calculation is executed for all the access types and the
33 consent patterns based on the assumption that the privacy
34 policy includes the elements shown in Figure 1, then it is

1 theoretically necessary to execute the preliminary calcula-
2 tion using the condition data for the following number of
3 times and store relevant results in the storage area:

4 [Formula 1]

5 The number of access types

6 = the number of kinds of the "data usage types"

7 [multiplied by]

8 the number of kinds of the "registrant data types"

9 [multiplied by]

10 the number of kinds of the "business purpose types"

11 [multiplied by]

12 the number of kinds of the "condition data" [multi-
13 plied by]

14 the record number of a client database (Formula 1)

15 Sufficient access management is achieved in the above-
16 described processes only if hardware resources such as a
17 storage capacity or processing speed used in an access
18 management system are sufficient for storing the above-
19 described data. However, according to the present
20 invention, it is possible to impart a wide range of appro-
21 priateness to the performances of the hardware resources by
22 compressing the registrant condition table corresponding to
23 the access types as will be described later. Now, the
24 above-mentioned compression processing for the access
25 authorization data in the present invention will be
26 described. The term "compression processing for the access
27 authorization data" in the present invention refers to
28 processing for deleting the registrant condition data which
29 are not accessed at least by judging from the privacy policy
30 when accessed and for generating a "disapproval list" at
31 least indicating the deleted registrant condition data.

32 Figure 6 shows reference axes applied when performing
33 the compression processing for the registrant condition
34 table contained in the access authorization data which are

1 usable in the access management method of the present inven-
2 tion. In the present invention, the registrant condition
3 table is regarded as a three-dimensional constitution having
4 three axes of an access type axis corresponding to the
5 records of the access type list, a condition data axis
6 corresponding to the number of the condition data, and a
7 registrant axis corresponding to the number of the regis-
8 trants. In the present invention, these axes are used as
9 the reference axes in the compression processing. When the
10 privacy policy shown in Figs. 2A to 2C is examined, it is
11 found that the appropriateness check can be executed with
12 judgment of the access type only, without referring to the
13 registrant condition table or the registrant condition data,
14 which are not usable at all or not necessary to use.

15 Specifically, when the data usage type is distribution
16 and the business purpose type is accounting, then the access
17 is judged to be disapproved, based on the setting of the
18 privacy policy without making reference to the registrant
19 condition table or executing the appropriateness check for
20 each piece of the condition data. Meanwhile, when the data
21 usage type is distribution and the business purpose type is
22 shipping, then there is a case where access authorization is
23 obvious at the point of policy setting with respect to the
24 addresses, the names, and the telephone numbers. Inciden-
25 tally, as for the condition data, it is possible to execute
26 the compression processing along with the respective corre-
27 sponding reference axes by focusing on the existence of a
28 certain classification in the registrant condition data,
29 such as a classification pattern for each condition data
30 where access by telephone is rejected but access by
31 electronic mail, facsimile or DM is accepted, or a classifi-
32 cation pattern depending on the registrants which tends to
33 reject unnecessary use of the sexes and the ages. In the
34 present invention, the above-described cases are referenced

1 as the processing for compression along the access type
2 axis, compression along the condition type axis, and
3 compression along the registrant axis. These compression
4 processes will be described in detail hereafter.

5 (Compression along the access type axis)

6 In particular, the access type axis in the present
7 invention is an axis corresponding to the records on the
8 access type list. In the compression processing for this
9 axis, the processing is carried out by classifying the sets
10 of the generated registrant condition table into the cases
11 where no access authorization is granted regardless of
12 executing the appropriateness check for the access types and
13 the cases where all kinds of access are authorized, and then
14 by registering those cases into an "authorization list" and
15 the "disapproval list" in advance. Figure 7 is a view
16 schematically showing this compression processing. As shown
17 in Figure 7, the registrant condition tables are created for
18 an access type 1 to an access type n which are given as a
19 multiplication of the number of the data usage types and the
20 number of the business purpose types. Among them, if assum-
21 ing that the access type 2 represents the data usage type of
22 distribution and also the business purpose type of account-
23 ing, for example, the result of the appropriateness check
24 will be always disapproval. Accordingly, it is unnecessary
25 to store the access type 2 into the storage area as a regis-
26 trant condition table. Therefore, the compression process-
27 ing is performed by deleting that table.

28 According to the present invention, the compression
29 processing is performed by deleting unnecessary registrant
30 condition tables and generating the disapproval list corre-
31 sponding to the deleted tables instead. In the embodiment
32 described in Figure 7, the access type 2 described above and
33 the access type 4 are added to the disapproval list 20.

1 Simultaneously, in Figure 7, the access type 1 and the
2 access type 3 can be classified as the access types, all of
3 which are authorized without sequential judgment of the
4 condition data. Accordingly, in Figure 7, the access type 1
5 and the access type 3 are registered in the authorization
6 list 22. For example, the access type 1 represents the data
7 usage type of "distribution" and the business purpose type
8 of "shipping". In this case, the privacy policy shows that
9 all the registrant IDs have agreed with access to the
10 addresses and the names which are required for shipping.
11 Accordingly, it is not necessary to execute the appropriate-
12 ness check when the registrant data contained in the access
13 request are just the addresses and the names. For this
14 reason, it is possible to add the access type 1 to the
15 authorization list.

16 Moreover, Figure 7 shows the processing to be executed
17 in the access management method of the present invention, in
18 which the appropriate check is executed comprising the steps
19 of deciding the access type by use of the authorization
20 engine when the access request arises, selecting the table
21 by use of a selection module, and making reference to the
22 disapproval list and the authorization list and thereby
23 executing the appropriateness check.

24 Figure 8 is a flowchart showing the processing to be
25 executed by the authorization engine when executing the
26 access management method of the present invention by use of
27 the data compression shown in Figure 7. In Step S50, the
28 authorization engine of the present invention receives an
29 access request from an application configured as another
30 software module separately from the authorization engine,
31 and executes data reading of the data usage type, the
32 business purpose type and the requested registrant data. In
33 Step S52, the access type is decided based on the data usage
34 type and the business purpose type which are read out in the

1 previous step. In Step S54, the disapproval list 20 is
2 firstly accessed to execute comparison of the obtained
3 access type so as to judge whether or not the decided access
4 type is registered in the disapproval list 20. In Step S54,
5 when the decided access type is registered in the disap-
6 proval list 20 (yes), it is not necessary to execute the
7 subsequent appropriateness check. Hence, access disapproval
8 is issued to the application.

9 Meanwhile, by the judgment of Step S54, when it is
10 found that the decided access type is not registered in the
11 disapproval list in Step S54 (no), access will be authorized
12 depending on the condition or without conditions. Accord-
13 ingly, the process continues to Step S56 for executing the
14 appropriateness check. On the contrary, when the decided
15 access type is registered in the disapproval list in Step
16 S54, the process continues to Step S58 and the access disap-
17 proval is returned to the application and the appropriate-
18 ness check is terminated at that point. Moreover, in
19 another embodiment of the access management method according
20 to the present invention, it is also possible to adopt the
21 processing in which the authorization list 22 is read out
22 first and the disapproval list 20 is referenced at a time
23 when the obtained access type is judged not to be regis-
24 tered in the authorization list 22.

25 (Compression processing along the condition data axis)

26 Figure 9 is a schematic drawing showing the compres-
27 sion processing along the condition data axis, which is
28 another embodiment of a data compression method of the
29 present invention. As shown in Figure 9, in a registrant
30 condition table corresponding an access type designated by
31 an access type axis i, it is assumed that all the regis-
32 trants agree with access to the names but do not agree with
33 access to the addresses of a relevant business purpose type.

1 In the compression processing along the condition data axis
2 of the present invention, an authorization list 24 and a
3 disapproval list 26 by the column are prepared and stored in
4 an appropriate storage area. Simultaneously, the columns
5 which are registered in the authorization 24 and the disap-
6 proval list 26 are deleted from the original registrant
7 condition table. Moreover, the condition data for different
8 columns are examined to judge as to whether or not all the
9 registrants register authorization or disapproval in the
10 same pattern. When all the registrants agree with the
11 authorization in the same pattern, then the columns are
12 integrated and indices are allocated to the integrated
13 columns for reference to the corresponding condition data.
14 After the above-described processes are executed, the access
15 authorization data of the present invention are finally
16 formed into a group of "the access type list, the compressed
17 registrant condition table, the authorization list, and the
18 disapproval list" and are stored in the storage area in a
19 format usable by the authorization engine.

20 Figure 10 is a flowchart showing the processing to be
21 executed by the authorization engine when using the access
22 authorization data after execution of the compression
23 processing along the condition data axis. According to the
24 processing shown in Figure 10, in Step S60, an access
25 request is received from an application configured as an
26 external function module, then the data usage type, the
27 business purpose type and the requested registrant data are
28 obtained and the access type is decided. In Step 62, the
29 access authorization data is referenced corresponding to the
30 obtained access type, and the authorization list or the
31 disapproval list is referenced. In Step S64, whether or not
32 the access type corresponding to the requested registrant
33 data is registered in each list is judged. When the corre-
34 sponding access type is registered in the authorization list

1 or the disapproval list (yes), the process continues to Step
2 S66 and access is controlled in accordance with the corre-
3 sponding list. On the contrary, when the corresponding
4 access type is not found in the authorization list or the
5 disapproval list in Step S64, the process continues to Step
6 S68 so that other appropriateness checks are executed.

7 (Compression processing along the registrant axis)

8 Figs. 11A to 11C describe an outline of the data
9 compression processing along the registrant axis used in the
10 present invention. In the privacy policy set by the policy
11 setter, there may be a case where identical authorization
12 judgment having a certain classification for the identical
13 data types is given even in the case of different regis-
14 trants. In this case, it is possible to compress the regis-
15 trant condition table by compressing the registrants for
16 each classification of the condition data. Specifically, as
17 shown in Figure 11A, for example, the registrants having the
18 registrant ID 002 and the registrant ID 004 have the identi-
19 cal consent condition data from the name to the mail and
20 thereby collectively constitute a classification.

21 Meanwhile, it is also possible to carry out similar
22 processing in column units. Figure 11B shows an
23 authorization/disapproval list of the registrants in column
24 units, and Figure 11C shows a list after the data compres-
25 sion executed by configuring the authorization/disapproval
26 list for each classification based on the records. In the
27 data compression along the registrant axis shown in Figs.
28 11A to 11C, all authorization/ disapproval data of the
29 registrants are registered in each list. Accordingly, the
30 authorization engine looks up in any of the list, then
31 executes the authorization judgment. The judgment process-
32 ing by the authorization engine in this embodiment can be
33 executed in a substantially similar manner to the example

1 embodiment of the present invention which utilizes the
2 access authorization data.

3 Moreover, in the access management method of this
4 embodiment as well, it is possible to adopt the configura-
5 tion in which the access authorization data is stored in a
6 high-speed cache memory together with a blank records and
7 sequentially added at runtime.

8 Figure 12 is a flowchart showing the processing for
9 adding and updating the access authorization data at
10 runtime, which can be executed when using the access
11 authorization data of the second embodiment of this inven-
12 tion. The processing for updating the access authorization
13 data at runtime shown in Figure 12 is started from Step S80,
14 in which whether or not there is a registrant condition
15 table corresponding to a certain access type is judged.
16 When the corresponding registrant condition table exists in
17 the judgment of Step S80 (yes), the process continues to
18 Step S82 and whether or not the access type to be judged is
19 registered in the authorization/disapproval lists.

20 In the judgment of Step S82, when the access type to
21 be judged is not included in the authorization/disapproval
22 list (no), the process continues to Step S84 and whether or
23 not the access type is registered in the
24 authorization/disapproval list generated along the condition
25 data axis. When the access type does not exist in the
26 authorization/disapproval list in the judgment of Step S86
27 (no), in Step S86, whether or not a cluster to be generated
28 along the registrant axis exists is judged. When the corre-
29 sponding access type does not exist either in the judgment
30 of Step S86 (no), the privacy policy data are read out and
31 the appropriateness check is executed in Step S86. Then, a
32 result of the check and the registrant ID are added to the
33 blank registrant condition table, and the process is
34 completed. On the contrary, when the corresponding

1 registrant condition table does not exist in the judgment in
2 Step S80 (no), then a corresponding registrant condition
3 table is generated in blank and stored in the storage area.
4 Then, the process is branched off to Step S82 and the next
5 authorization judgment is executed.

6 Meanwhile, when it is judged that the access type
7 belongs to the authorization/disapproval list in the
8 judgment of Step S82 (yes), the process continues to Step
9 S92 and consistency between the authorization/disapproval
10 list and the registrant condition table is checked, and then
11 the process is branched off to the judgment of Step S84. In
12 the present invention, the processing for checking the
13 consistency refers to the processing including the steps of
14 judging whether or not the access authorization obtained by
15 use of the authorization/disapproval list conflicts with the
16 result given by the registrant condition table, deleting the
17 access authorization generated by the authorization/disap-
18 proval list in case of a conflict, and modifying the access
19 authorization into proper access authorization and storing
20 the proper access authorization. Moreover, when it is
21 judged that the access type belongs to the
22 authorization/disapproval list in the judgment of Step S84
23 (yes), the process continues to Step S94 where consistency
24 between the authorization/disapproval list and the regis-
25 trant condition table is checked and the process is further
26 branched off to the judgment of Step S86. Furthermore, when
27 it is judged that there is a cluster of the corresponding
28 access type in the judgment of Step S86 (yes), the corre-
29 sponding registrant ID is added by use of a result of execu-
30 tion of the appropriateness check for the cluster, and the
31 process is completed.

32 It is not always necessary to select any one mode of
33 the compression processing described above. It is possible
34 to execute the data compression in combination of a

1 plurality of the above-described modes as needed. For
2 example, it is possible to execute the compression process-
3 ing along the condition data axis after executing the
4 compression processing along with the access type axis so as
5 to perform the compression processing along the condition
6 axis for the columns which are not included in the authori-
7 zation list or the disapproval list. Thereafter, the
8 compression processing is executed along the registrant axis
9 for each record. In this way, it is possible to considera-
10 bly reduce the overhead for the appropriateness checks to be
11 executed by the authorization engine after receiving the
12 access request from the application.

13 Section B: Implementation of the access management method
14 of the present invention

15 The access management system of the present invention
16 is configured as a computer-executable program. The
17 computer-executable program recorded in a computer-readable
18 recording medium or a transmission medium is installed in a
19 computer system so as to cause the computer to achieve the
20 respective functions described above. Now, processing to be
21 performed will be explained when the access management
22 system of the present invention is implemented in the
23 computer system. Hereafter, the most basic access manage-
24 ment system is assumed for explanation. However, it is to
25 be noted that similar functions can be configured over
26 appropriate constituents even in the access management
27 method or access management system mutually connected via a
28 network respectively.

29 Figure 13 shows primary processing of the access
30 management method of the present invention prior to starting
31 the process. This processing can be executed by a prelimi-
32 nary calculation unit configured in any of computers in the
33 system. In the primary processing shown in Figure 13, in

1 Step S100, the preliminary calculation unit is caused to
2 read the privacy policy data which are set up by the policy
3 setter. It is also possible to execute such a storing
4 method by reading the privacy policy stored in any of
5 storage units in the system. Alternatively, the person in
6 charge at the policy setter can perform input and storage
7 according to an appropriate method.

8 In Step S102, either generation of the cluster value
9 or the compression processing is executed in response to the
10 format of the access authorization data to be used, whereby
11 the above-described access authorization data including the
12 access type list and the registrant condition table are
13 created and stored in the storage area. As another embodi-
14 ment, it is also possible to store the access type list, the
15 registrant condition table, the condition logic, and the
16 selection logic into a memory area which the authorization
17 engine and a creation unit can share. As further another
18 embodiment where the authorization engine and the creation
19 unit are remotely connected to each other through a network,
20 it is possible to transmit the access type list, the regis-
21 trant condition table, the condition logic, the selection
22 logic, and the like are transferred to and stored in the
23 authorization engine, or it is also possible for the
24 authorization engine to make reference to the access type
25 list, the registrant condition table, the condition logic,
26 the selection logic, and the like stored in the creation
27 unit and to perform the processing.

28 In Step S104, the authorization engine is caused to
29 start the processing for the appropriateness checks and to
30 manage access to the registrant database in response to the
31 access request from the application. In Step S106, a
32 monitoring unit causes the authorization engine to continu-
33 ously or sequentially monitor as to whether there is a
34 change in the condition type such as consent by the

1 registrant or a change in the contents of policies on the
2 policy setter's side. Results of judgment in Step S106 are
3 sent to Step S108. When it is judged that any of the data
4 is updated in Step S108 (yes), the process continues to Step
5 S110 where the portion in the access type list, the regis-
6 trant condition table, the condition logic, the selection
7 logic, or the like to be changed is specified, and the
8 preliminary calculation unit executes recalculation.

9 In Step S112, the recalculated portion out of the
10 access type list, the registrant condition table, the condi-
11 tion logic, the selection logic, and the like is stored in
12 an appropriate storage area as usable by the authorization
13 engine. Then the process returns to Step S104 and the
14 processing by the access management system is executed
15 continuously. Meanwhile, when it is judged that there are
16 no updates as a result of the judgment of Step S108 (no),
17 the existing access type list, the registrant condition
18 table, the condition logic, the selection logic, and the
19 like are usable directly. Accordingly, the process returns
20 to Step S104 without updating the access authorization data
21 and the processing by the access management system is
22 executed.

23 Figure 14 shows the processing by the access manage-
24 ment method of another embodiment where the registrant
25 condition table is dynamically added instead of being
26 created in advance. In the embodiment shown in Figure 14,
27 the authorization engine receives the access request to the
28 registrant data from the application and thereby obtains the
29 access type in Step S114. In Step S116, the authorization
30 engine searches the access type list and the registrant
31 condition table, and judges whether or not the obtained
32 access type is found in the access authorization data. When
33 no data corresponding to the registrant condition table are
34 found in the judgment of Step S116 (no), the process

1 continues to Step S118 and the authorization engine notifies
2 the preliminary calculation unit of the absence of a result
3 corresponding to the access authorization and of the
4 requested access type. In Step S120, the preliminary calcu-
5 lation unit accesses the registrant database and extracts
6 the registrants corresponding to the access type. Then, the
7 preliminary calculation unit executes the appropriateness
8 checks by comparing the registrant data with the private
9 policy to generate the cluster identification value. Subse-
10 quently, the preliminary calculation unit registers the
11 cluster identification value as a new record in the regis-
12 trant condition table. In Step S122, the creation unit
13 returns the whole part of or the updated part of the created
14 access authorization data to the authorization engine, and
15 causes the authorization engine to execute the appropriate-
16 ness checks.

17 Meanwhile, when the data corresponding to the regis-
18 trant condition table are found in the judgment of Step
19 S116, it is possible to complete the appropriate checks for
20 the access request which is evaluated at that point by means
21 of only making reference to the cluster identification value
22 obtained already by executing the appropriateness checks.
23 In the embodiment shown in Figure 14, the appropriateness
24 checks of the condition data are performed at runtime.
25 Accordingly, although it takes more time to receive the
26 results on the application side as compared to the embodi-
27 ment described in Figure 14, it is possible to impart the
28 same efficiency as that described in Figure 14 when the
29 registrant condition table is once configured. Moreover, in
30 order to accelerate this processing, it is also possible to
31 construct the registrant condition table sequentially in the
32 cache memory.

33 Figure 15 is a view showing an aspect of the process-
34 ing for dynamically adding the record when creating the

1 registrant condition table for each access type in the
2 access management method according to the second embodiment
3 of the present invention. In Figure 15, the authorization
4 engine received the access request to the registrant data
5 from the application to thereby decide the access type in
6 Step S130. In Step S132, the access type list is refer-
7 enced while using the decided access type and the requested
8 registrant data as keys, and whether or not the decided
9 access type exists in the access type list is judged. When
10 the access type list is found in the judgment of Step S132
11 (yes), the process continues to Step S134 and judgment for
12 access authorization is executed by use of the corresponding
13 registrant condition table. Then access control to the
14 registrant database is executed in Step S140 based on a
15 result thereof. Thereafter, the process returns to Step
16 S130 for standing by for a subsequent access request.

17 On the contrary, when the access type judged at that
18 moment is not found in the access type list in the judgment
19 of Step S132 (no), the process continues to Step S136 and
20 the authorization engine passes the notification of absence
21 of the access type and the relevant access type to the
22 creation unit. In Step S138, the preliminary calculation
23 unit executes the appropriateness check by use of the
24 privacy policy data and creates a new record for the access
25 authorization data together with a result of the appropri-
26 ateness check. Then, the preliminary calculation unit
27 stores the access authorization data in the storage area as
28 a format usable by an evaluation engine. In Step S140, the
29 evaluation engine executes the appropriateness check by use
30 of the newly obtained record, and a result thereof is
31 returned to the application.

32 Section C: The access management system of the present
33 invention

1 Figure 16 is a schematic functional block diagram
2 showing the access management system according to the
3 present invention where the access management method of the
4 present invention is implemented. As shown in Figure 16, an
5 access management system 30 of the present invention
6 includes an authorization engine 34 for receiving an access
7 request from an application execution unit 32 and for
8 executing processing, a preliminary calculation unit 38, and
9 a storage area 40. The authorization engine 34 includes an
10 authorization judgment unit 36 for processing access
11 authorization judgment. The application execution unit 32
12 receives an input from the person in charge and issues the
13 access request to the authorization engine 34 by use of an
14 SQL sentence or the like. Moreover, the application execu-
15 tion unit 32 also executes processing for receiving a result
16 from the authorization engine and returning the result to
17 the person in charge. The application execution unit 32 is
18 configured as capable of carrying out prescribed operations
19 by causing a computer to execute either specific or general
20 operation software related to the operation required by the
21 policy setter.

22 The authorization engine 34 receives the access
23 request and reads data such as a data usage type, a business
24 purpose type, or requested registrant data contained in the
25 access request. Then, the authorization engine 34 decides a
26 requested access type from the data thus read out, and
27 stores the access type in a memory area 40 properly consti-
28 tuted including a hard disk, a high-speed access memory (a
29 cache memory). Meanwhile, the preliminary calculation unit
30 38 reads a privacy policy stored in a privacy policy
31 database 42 and registrant data stored in a registrant
32 database 44, and creates access authorization data in
33 advance including an access type list and a registrant
34 condition table. The access authorization data thus created

1 are stored in the memory area 40, for example. In this
2 case, the memory area 40 may include a database which is
3 configured by appropriate software.

4 The created access authorization data including the
5 access type list and the registrant condition table are
6 stored in the memory area 40 once, and then are made
7 readable by the authorization engine 34. Simultaneously,
8 when it is necessary to provide selection logic for the
9 registrant condition table, the preliminary calculation unit
10 38 stores such selection logic simultaneously in the memory
11 area 40.

12 The access management system of the present invention
13 will be explained with reference to Figure 16 again. A
14 monitoring unit 46 constituting the access management system
15 30 monitors changes and updates of the data in the privacy
16 policy database 42 and the registrant database 44.
17 Moreover, the monitoring unit 46 monitors consistency of the
18 data between the privacy policy database 42 of the regis-
19 trant database 44 periodically or continuously, for example.
20 When the registrant changes setting for the condition data
21 or when a new registrant record is added, for example, the
22 monitoring unit 46 extracts a conflicted part of the data to
23 thereby judge the change in the setting of the condition
24 data or the addition of the new registrant record. When the
25 monitoring unit 46 judges that there is the change in
26 setting of the condition data or the addition of the new
27 registrant record, the monitoring unit 46 transmits the
28 changed condition type or the new registrant record to the
29 preliminary calculation unit 38. Upon receipt of the data,
30 the preliminary calculation unit 38 creates access authori-
31 zation data corresponding to the data and stores difference
32 data in the storage area 40 so that the authorization engine
33 34 can execute the processing inclusive of the new regis-
34 trant data.

1 Figure 17 is a view showing the access management
2 system according to the second embodiment of the present
3 invention. Figure 17 is the view of the access management
4 system of the second embodiment of the present invention
5 which shows a configuration in the case of performing data
6 compression along an access type axis, a condition data
7 axis, or a registrant axis. The access management system 30
8 of the present invention includes the authorization engine
9 34, the preliminary calculation unit 38, and the storage
10 area 40. The authorization engine 34 further includes the
11 authorization judgment unit 36 and a selection module 48 for
12 executing judgment to select each table or list in the
13 access authorization data. The application execution unit
14 32 executes the processing substantially similar to that
15 described in Figure 16, and also executes processing for
16 returning a result given by access management to the person
17 in charge.

18 The authorization engine 34 receives the access
19 request and reads the data such as the data usage type, the
20 business purpose type, or the requested registrant data
21 contained in the access request. Then, the authorization
22 engine 34 decides the requested access type from the data
23 thus read out. Meanwhile, the preliminary calculation unit
24 38 reads the privacy policy stored in the privacy policy
25 database 42 and the registrant data stored in the registrant
26 database 44, and creates selection logic to enable reference
27 to an authorization/disapproval list or table generated by
28 performing compression processing of the access type list,
29 the registrant condition table and compression data corre-
30 sponding thereto, and the like. The preliminary calculation
31 unit 38 stores the selection logic in the memory area 40
32 appropriately constituted including a hard disk, a high-
33 speed access memory (a cache memory).

34 The selection module 48 receives the decided access

1 type and simultaneously reads the selection logic and the
2 access authorization data out of the storage area 40, and
3 then passes the access authorization data to the authoriza-
4 tion judgment unit. The authorization engine 34 enables
5 judgment of authorization or disapproval of the access to
6 the registrant database by use of the access request and the
7 access authorization data thus received. When access is
8 authorized, the application execution unit 32 can obtain the
9 corresponding registrant data. On the contrary, when access
10 is not authorized, the application execution unit 32
11 receives notification of access disapproval from the
12 authorization engine 34.

13 Figure 18 is a view showing an access management
14 system according to a third embodiment of the present inven-
15 tion. An access management system 50 shown in Figure 18 is
16 a system configured to manage access to the registrant data
17 through a network such as a local area network (LAN) or a
18 wide area network (WAN). The access management system 50
19 shown in Figure 18 includes a network 52, a plurality of
20 application computers 54 connected to the network 52, the
21 registrant database 44, and the privacy policy database 42.
22 In the embodiment described herein, the registrant database
23 44 and the privacy policy database 42 are managed by a
24 management server 56. Moreover, the management server 56
25 includes the function as the preliminary calculation unit
26 38, the function as the monitoring unit 46, and the function
27 as the storage area 40 as described in Figure 16 and Figure
28 17. The management server 56 is capable of calculating in
29 advance and storing the data necessary for executing the
30 access management method of the present invention, such as
31 the access type list, the registrant condition table, or the
32 selection logic. Meanwhile, in the embodiment shown in
33 Figure 18, each application computer 54 includes the appli-
34 cation execution unit 32 and the authorization engine 34.

1 The access management data required for authorization
2 judgment processing are transmitted to the authorization
3 engine 34 as shown in Figure 18 from the management server
4 56 together with data for the selection logic. The data are
5 stored in an appropriate storage area contained in the
6 application computer 54. Each application computer 54 is
7 constituted in such a way that the access request is
8 subjected to the processing of the application computer 64
9 by use of the stored access authorization data and the
10 access request, and access to the registrant database is
11 controlled by the authorization engine 34. The authoriza-
12 tion engine 34 processes the access request based on the
13 above-described access management method of the present
14 invention, and transmits only the access request which
15 passed the appropriateness check to the management server
16 56. The management server 56 searches and extracts the
17 requested registrant data out of the registrant database 42,
18 and passes the registrant data to the application computer
19 54.

20 Incidentally, in another embodiment of the present
21 invention, an authorization server (not shown) can be
22 configured separately without providing the application
23 computer 54 with the function as the authorization engine.
24 Meanwhile, the authorization engine can be configured
25 separately from the management server 56 as a gateway server
26 for processing the access request from the application
27 computer 54. In this way, it is possible to process the
28 access requests from the plurality of application computers
29 54 independently of the preliminary calculation function.

30 Although the present invention has been described
31 based on certain embodiments shown in the accompanying
32 drawings, it is not limited to the particular embodiments
33 described herein. Moreover, it is to be noted that the
34 access management method of the present invention can be

1 written as computer-executable programs using various
2 programming languages. Such programming languages include C
3 Language, C++ Language, Java (trademark), and the like.
4 Furthermore, the computer-readable programs for executing
5 the access management method of the present invention can be
6 stored in various recording media for distribution, such as
7 a ROM, an EEPROM, a flash memory, a CD-ROM, a DVD, a flexi-
8 ble disk, or a hard disk.

9 Application of the present invention can accelerate an
10 appropriateness check of a privacy policy without damaging
11 reliability. Particularly, the overhead of the appropriate-
12 ness checks constituted a large problem in an application
13 configured to obtain a large amount of information at a
14 time. However, the present invention is particularly effec-
15 tive in such a system accompanying the large amount of data
16 access.

17 Although the preferred embodiments of the present
18 invention have been described in detail, it should be under-
19 stood that various changes, substitutions and alternations
20 can be made therein without departing from spirit and scope
21 of the invention as defined by the appended claims. Varia-
22 tions described for the present invention can be realized in
23 any combination desirable for each particular application.
24 Thus particular limitations, and/or embodiment enhancements
25 described herein, which may have particular advantages to
26 the particular application need not be used for all applica-
27 tions. Also, not all limitations need be implemented in
28 methods, systems and/or apparatus including one or more
29 concepts of the present invention.

30 The present invention can be realized in hardware,
31 software, or a combination of hardware and software. A
32 visualization tool according to the present invention can be
33 realized in a centralized fashion in one computer system, or
34 in a distributed fashion where different elements are spread

1 across several interconnected computer systems. Any kind of
2 computer system - or other apparatus adapted for carrying
3 out the methods and/or functions described herein - is
4 suitable. A typical combination of hardware and software
5 could be a general purpose computer system with a computer
6 program that, when being loaded and executed, controls the
7 computer system such that it carries out the methods
8 described herein. The present invention can also be embed-
9 ded in a computer program product, which comprises all the
10 features enabling the implementation of the methods
11 described herein, and which - when loaded in a computer
12 system - is able to carry out these methods.

13 Computer program means or computer program in the
14 present context include any expression, in any language,
15 code or notation, of a set of instructions intended to cause
16 a system having an information processing capability to
17 perform a particular function either directly or after
18 conversion to another language, code or notation, and/or
19 reproduction in a different material form.

20 Thus the invention includes an article of manufacture
21 which comprises a computer usable medium having computer
22 readable program code means embodied therein for causing a
23 function described above. The computer readable program
24 code means in the article of manufacture comprises computer
25 readable program code means for causing a computer to effect
26 the steps of a method of this invention. Similarly, the
27 present invention may be implemented as a computer program
28 product comprising a computer usable medium having computer
29 readable program code means embodied therein for causing a a
30 function described above. The computer readable program
31 code means in the computer program product comprising
32 computer readable program code means for causing a computer
33 to effect one or more functions of this invention. Further-
34 more, the present invention may be implemented as a program

1 storage device readable by machine, tangibly embodying a
2 program of instructions executable by the machine to perform
3 method steps for causing one or more functions of this
4 invention.

5 It is noted that the foregoing has outlined some of
6 the more pertinent objects and embodiments of the present
7 invention. This invention may be used for many
8 applications. Thus, although the description is made for
9 particular arrangements and methods, the intent and concept
10 of the invention is suitable and applicable to other
11 arrangements and applications. It will be clear to those
12 skilled in the art that modifications to the disclosed
13 embodiments can be effected without departing from the
14 spirit and scope of the invention. The described embodi-
15 ments ought to be construed to be merely illustrative of
16 some of the more prominent features and applications of the
17 invention. Other beneficial results can be realized by
18 applying the disclosed invention in a different manner or
19 modifying the invention in ways known to those familiar with
20 the art.